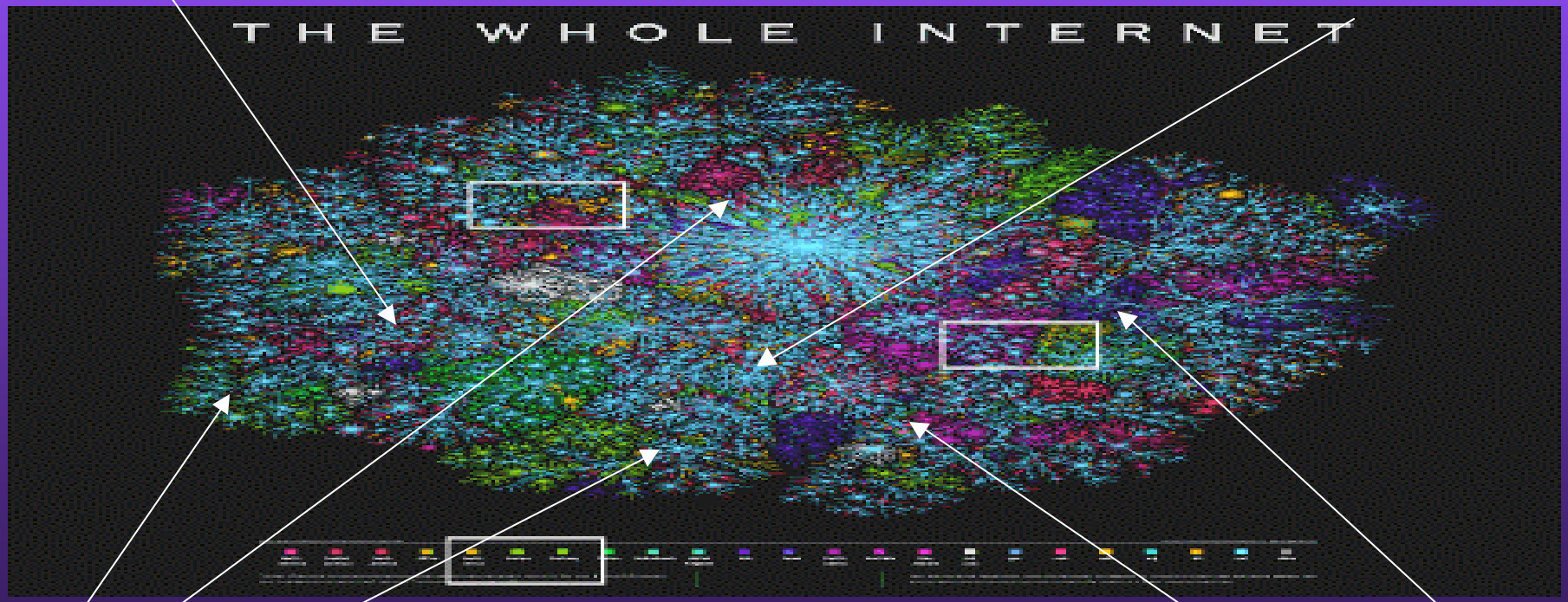
# INFORMATION WARFARE

## Sharing: Basis for Partnership

## National Security in the Interconnected Age

USA.gov/mil ?

USA.com/org ?




NATO - Friends ?

China - Others ?

**Dr Dan Kuehl "kuehld@ndu.edu"**

**Information Resources Management College**

**National Defense University**

**"My opinions: not necessarily the USG, DOD, or NDU!"**

# Scenario for a New Paradigm

- "Reston Telematics"
  - "If the byte's important, we handle it!"
  - Economic, Military, Political
- Wartime = target
- Who defends it against enemy…
  - Military / air force, navy, army, space?
    - DOD/uniformed military/national security!
  - Cyber?
    - Hmmmmm…

# 4 Fundamental Changes

- New geostrategic context
  - Cyberspace: new operational realm
    - Dominant in business, politics, warfare
  - Convergence
    - Digital: 1110101110001010 = lingua franca
  - Omnilinking
    - Worldwide electronic digital connectivity of people, organizations, governments…Instantly & Globally
  - Infrastructures controlled by computer
    - Opportunity….and vulnerability
    - Owned/operated by private sector
- Information power & national security

# Thesis #1
# “the battlespace”

- Information
  - Weapon - Tool - Process - Target
    - more than aid to “Blast - Heat - Fragmentation”
      - LTG Mike Hayden, DirNSA
- Synergy
  - human factors **+** information technology
- Information
  - element of national power
  - operational environment

# Thesis #2
# “the threat”

- Modern societies are increasingly vulnerable
  - Technologically/Economically
    - Infrastructures
      - telecommunications, energy, transportation, etc
  - Socially/Politically
    - Perception management, politics
      - “CNN Effect”, “strategic influence”, Al Jazeera, etc
- Access requires BOTH technological capability AND political acceptance
  - these are different vulnerabilities
  - Halt forces as far from the battlespace as possible

# Thesis #3
# “the partnership”

- The Department of Defense (or MOD), Federal Government, and the private sector share
  - Roles
  - Responsibilities

In protecting, leveraging, exploiting:
“national cyberspace” & information power

# Critical Infrastructure Protection

- PCCIP to PDD 63 to National Plan to EO 13231 (CIP in Info Age)
  - Next?
  - Australia, Russia, Norway, Sweden, Canada, more
- Dependency creates the Vulnerability
  - economic, political, societal, military

# Information COGs

- Critical infrastructures that support national power
  - Economic, Military, Diplomatic, Informational
    - RR, electricity, ATC, telecomms, etc
    - Crucial (hidden) role of private sector
- “Softpower”
  - Perceptions of America – global and domestic
    - Media, websites, radio, TV, etc
    - Serbian media vs NATO cohesion 1999
- Joint Vision requires Information Superiority
  - “reachback”, ISR, targeting, C2
  - Tanker-Airlift Control Center, Logistics C2

# Chinese IW

- Distinctions between levels of war and front and rear will disappear
  - **Weapons will "reach over the horizon and cross national boundaries [to attack] command centers, C3 hubs, info processing centers..and supply systems**
  - **"soft" [EW/IW] replacing "hard strike forces" to "interfere with/destroy other side's info and cognitive systems"**
    - Chen Huan, "The Third Military Revolution", in Chinese Views of Future Warfare, www.ndu.edu

# Evolving Changes

- Homeland Security
  - Cybersecurity: partnerships with whom?
    - Defensive IW within CIP: DOD roles/missions?
  - Information or Intelligence?
    - Different rules, equities, organizations
  - Focus
    - National problem…or insoluble without the international perspective?
      - International Law, Regional perspectives (ie. European Union), United Nations

# Partners Must Share

- Factors critical to success
  - Foster trust & respect
  - Communications: timely, secure, etc
  - Top management must support
  - Continuity of leadership
  - Member benefits
    - **GAO 02-24 “Info Sharing: practices that can benefit CIP “**

# Partners Must Share

- Challenges
  - Initial trust bond difficult
  - Need for agreements
  - Funding
  - Develop & Maintain member base
  - Develop & Maintain skills
    - **GAO 02-24 “Info Sharing: practices that can benefit CIP”**

# Partners Must Share

- Organizations doing it
  - Agora (Pacific NW) -- CDC
  - CERT Coordination Center -- FedCIRC
  - International Info Integrity Institute
  - InfraGard - JTF-CNO – NY Electronic Crimes Task Force - North Am Electric Reliability Cncl
  - National Coord Center for Telecomms
  - Network Security Info Exchanges
    - **GAO 02-24 “Info Sharing: practices that can benefit CIP”**

# A FEW ANSWERS…….
# MANY MORE QUESTIONS!